PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-115167
(43)Date of publication of application : 21.04.2000

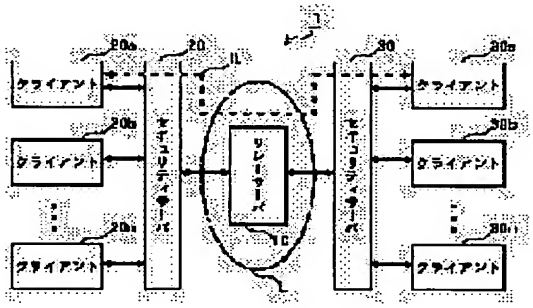
(51)Int.Cl. H04L 12/22
H04L 12/56

(21)Application number : 10-286508
(22)Date of filing : 08.10.1998

(71)Applicant : NTT DATA CORP
DOWANGO:KK
(72)Inventor : HIRAO YOSHIKUNI
KAWAKAMI KAZUO

(54) DATA COMMUNICATION METHOD, DATA REPEATER AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a data communication system capable of performing real time communication even under the environment when direct data communication with an opposite side is limited.
SOLUTION: Between clients 20a-20n under security servers 20 and 30 for allowing the transmission of only the communication data of a prescribed form such as a firewall and the clients 30a-30n under the security server 30, a relay server 10 for relaying the communication data between the clients is provided. The relay server 10 performs the pseudo exchange of the communication data from the client 20a to a data form whose transmission is allowed by the security server 30 provided with the client 30a of a communicating opposite party as a subordinate and transmits it to the client 30a.



LEGAL STATUS

[Date of request for examination]	16.11.1998
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	2998839
[Date of registration]	05.11.1999
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－115167
（P2000－115167A）
(43)公開日　平成12年４月21日(2000.4.21)

(51)Int.Cl.'	識別記号	Ｆ Ｉ		テーマコード'（参考）
Ｈ０４Ｌ　12/22		Ｈ０４Ｌ　11/26		５Ｋ０３０
12/56		11/20	１０２Ｚ	９Ａ００１

審査請求　有　　請求項の数10　ＯＬ　（全 10 頁）

(21)出願番号　特願平10－286508

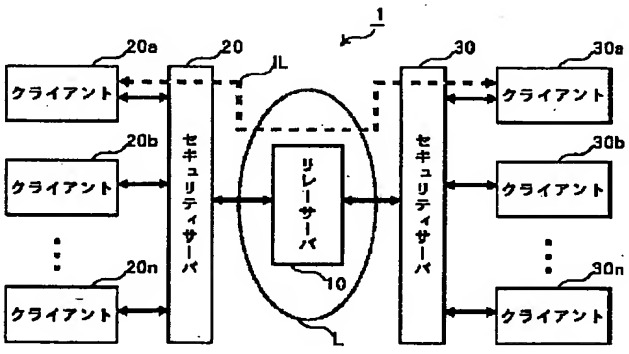
(22)出願日　平成10年10月８日(1998.10.8)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(71)出願人　598138327
株式会社ドワンゴ
東京都中央区日本橋人形町２－14－６　セルバ人形町
(72)発明者　平尾　吉邦
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100099324
弁理士　鈴木　正剛

最終頁に続く

(54)【発明の名称】　データ通信方法、データ中継装置及び記録媒体

(57)【要約】
【課題】　相手側との間の直接的なデータ通信が制限される環境下においてもリアルタイム通信を行うことができるデータ通信システムを構築する。
【解決手段】　ファイアウォール等の所定形式の通信データのみの透過を許容するセキュリティサーバ２０，３０の配下にあるクライアント２０ａ～２０ｎと、セキュリティサーバ３０の配下にあるクライアント３０ａ～３０ｎとの間に、クライアント間の通信データを中継するリレーサーバ１０を設ける。このリレーサーバ１０は、クライアント２０ａからの通信データを通信相手先のクライアント３０ａを配下にもつセキュリティサーバ３０が透過を許容するデータ形態に擬似的に交換し、これをクライアント３０ａ宛に送信する。



【特許請求の範囲】
【請求項１】　配下にある１又は複数の通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置が介在する環境下で行うデータ通信方法であって、
外部装置から特定の前記通信装置宛に送信された通信データを前記透過許容データに擬似的に変換して当該セキュリティ装置を透過させることを特徴とする、データ通信方法。
【請求項２】　前記外部装置、セキュリティ装置及び前記特定の通信装置をそれぞれ登録しておき、登録された外部装置から登録された通信装置宛の通信データのみを前記透過許容データに擬似的に変換して前記登録されたセキュリティ装置を透過させることを特徴とする、請求項１記載のデータ通信方法。
【請求項３】　それぞれ配下にある１又は複数の通信装置との間で所定形態の透過許容データのみの透過を許容する複数のセキュリティ装置が介在する環境で行うデータ通信方法であって、
特定のセキュリティ装置の配下にある第１通信装置から他のセキュリティ装置の配下にある第２通信装置宛の通信データを当該他のセキュリティ装置用の前記透過許容データに擬似的に変換して当該他のセキュリティ装置を透過させることを特徴とする、データ通信方法。
【請求項４】　前記通信データまたは透過許容データを前記第２通信装置毎に一時的に保持しておき、前記第２通信装置からの要求を契機に当該通信データについてはそれを前記他のセキュリティ装置用の透過許容データに擬似的に変換し、前透過許容データについてはそれを当該第２通信装置宛に送信することを特徴とする、請求項３記載のデータ通信方法。
【請求項５】　配下にある通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置と外部装置との間に介在し、
前記外部装置、前記セキュリティ装置及びこのセキュリティ装置の配下にある相手側通信装置を登録する登録手段と、
前記登録された外部装置から前記登録された相手側通信装置宛の通信データを登録された前記セキュリティ装置用の透過許容データに変換するデータ変換手段と、
前記擬似的に変換された透過許容データの前記登録された相手側通信装置による取得を許容する手段とを備えて成る、データ中継装置。
【請求項６】　前記相手側通信装置毎のデータ記憶領域を有し、前記通信データ変換手段は、保持されている前記通信データを前記相手側通信装置からの要求を契機に前記透過許容データに擬似的に変換することを特徴とする、請求項５記載のデータ中継装置。
【請求項７】　前記データ変換手段は、前記通信データのヘッダ部分に、当該通信データが前記相手側通信装置からの要求に応じたものであり且つＨＴＴＰまたはＳＭＴＰに従うデータである旨の情報を付加することで当該通信データを擬似的に前記透過許容データに変換することを特徴とする、
請求項６記載のデータ中継装置。
【請求項８】　前記外部装置が、前記セキュリティ装置と同種の機能を有する他のセキュリティ装置の配下にある通信装置であることを特徴とする、
請求項５記載のデータ中継装置。
【請求項９】　前記セキュリティ装置及び前記他のセキュリティ装置と共に、ＴＣＰ／ＩＰに準拠した公衆通信網に接続されることを特徴とする、
請求項８記載のデータ中継装置。
【請求項１０】　配下にある通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置と外部装置の各々に対するデータ通信機能を具備したコンピュータ装置に、少なくとも、
前記外部装置、前記セキュリティ装置及びそのセキュリティ装置の配下にある相手側通信装置を登録する処理と、
前記登録された外部装置から前記登録された相手側通信装置宛の通信データを擬似的に前記透過許容データに変換する処理と、
前記擬似的に変換された透過許容データの前記登録された相手側通信装置による取得を許容する処理とを実行させるためのプログラムが記録された、
コンピュータ読取可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、通信装置間のデータ交換方法等に関し、特に、所定の通信形式の通信データのみの透過を許容するセキュリティ装置の配下にある通信装置と、外部装置、例えば他の独立したセキュリティ装置の配下にある通信装置との間で、ネットワーク上に配置されたデータ中継装置を介して行うデータ通信方法及びその関連技術に関する。
【０００２】
【従来の技術】近年、インターネット等の不特定者が利用可能なネットワークを介してデータ通信を行う際のセキュリティ性を高めるために、当該ネットワークにセキュリティ装置を設けることが一般化している。この種のセキュリティ装置は、例えば配下にある通信装置とネットワークとの間に例えばファイアウォール等を設け、電子メールやホームページデータのような所定形態のデータのみの透過を許容し、それ以外のデータの透過を阻止する機能を有するものである。このようなセキュリティ装置において、インターネットにおけるサーバ機能を有するものは、セキュリティサーバと呼ばれている。
【０００３】インターネットにこのようなセキュリティサーバを設けることは、配下の通信装置に対する不特定

者の有害なアクセスを排除し得る利点はあるが、以下のような問題も生じる。すなわち、ある通信装置と他の独立したセキュリティサーバの配下にある通信装置との間で、リアルタイム通信、例えば対戦型ゲームやリアルタイムチャットサービス等を行おうとしても、セキュリティサーバが介在するためにそれができない。すなわち、一方の通信装置から他方の通信装置に通信するためのセッション（論理回線路、以下同じ）を確立しようとしても、いずれかのセキュリティサーバ又は双方のセキュリティサーバによって、セッション確立が拒否されてしまう。これは、セキュリティサーバが、通信装置とネットワーク間のパケットを直接透過させずに間接経路でのみ透過を許容することで、配下の通信装置を保護しているためである。

【０００４】そこで本発明は、相手側との間の直接的なデータ通信が制限される環境下においても、必要に応じてリアルタイム通信乃至それに近似した通信を行うことができる、改良されたデータ通信方法を提供することを課題とするものである。本発明の他の課題は、上記データ通信方法を実現するためのデータ中継装置、及び、上記データ通信方法をコンピュータ装置上で実行するための記録媒体を提供することにある。

【０００５】

【課題を解決するための手段】上記課題を解決する本発明のデータ通信方法は、配下にある１又は複数の通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置が介在する環境下で行うデータ通信方法であって、外部装置から特定の前記通信装置宛に送信された通信データを前記透過許容データに擬似的に変換して当該セキュリティ装置を透過させることを特徴とする。好ましくは、前記セキュリティ装置及び前記特定の通信装置を予め登録しておき、登録した通信装置宛の通信データのみを前記透過許容データに擬似的に変換して登録されたセキュリティ装置を透過させるようにする。

【０００６】前記セキュリティ装置が複数介在する環境でデータ通信を行う場合は、特定のセキュリティ装置の配下にある第１通信装置から他のセキュリティ装置の配下にある第２通信装置宛の通信データを当該他のセキュリティ装置用の前記透過許容データに擬似的に変換して当該他のセキュリティ装置を透過させる。なお、前記通信データまたは透過許容データを前記第２通信装置毎に一時的に保持しておき、前記第２通信装置からの要求を契機に当該通信データについてはそれを前記他のセキュリティ装置用の透過許容データに擬似的に変換し、前透過許容データについてはそれを当該第２通信装置宛に送信するようにしてもよい。

【０００７】上記他の課題を解決する本発明のデータ中継装置は、配下にある通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置と外部装置との間に介在するもので、前記外部装置、前記セキュリティ装置及びこのセキュリティ装置の配下にある相手側通信装置を登録する登録手段と、前記登録された外部装置から前記登録された相手側通信装置宛の通信データを擬似的に登録された前記セキュリティ装置用の透過許容データに変換するデータ変換手段と、前記擬似的に変換された透過許容データの前記登録された相手側通信装置による取得を許容する手段とを備えて構成したものである。

【０００８】前記データ変換手段は、例えば、前記通信データのヘッダ部分に、当該通信データが前記相手側通信装置からの要求に応じたものであり且つＨＴＴＰ（HyperText Transfer Protocol）またはＳＭＴＰ（Simple Mail Trasfer Protocol）に従うデータである旨の情報を付加することで当該通信データを擬似的に前記透過許容データに変換するように構成する。

【０００９】上記他の課題を解決する本発明の記録媒体は、配下にある通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置と外部装置の各々に対するデータ通信機能を具備したコンピュータ装置に、少なくとも下記の処理を実行させるためのプログラムが記録された、コンピュータ読取可能な記録媒体である。

（１）前記外部装置、前記セキュリティ装置及びそのセキュリティ装置の配下にある相手側通信装置を登録する処理、

（２）前記登録された外部装置から前記登録された相手側通信装置宛の通信データを擬似的に前記透過許容データに変換する処理、

（３）前記擬似的に変換された透過許容データの前記登録された相手側通信装置による取得を許容する処理。

【００１０】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を詳細に説明する。図１は、本発明を適用したデータ通信システムの概略構成図である。このデータ通信システム１は、セキュリティサーバ２０の配下にある複数の通信装置（以下、通信装置を「クライアント」と称する）２０ａ～２０ｎと、他の独立したセキュリティサーバ３０の配下にある複数のクライアント３０ａ～３０ｎを、インターネットＬ上のリレーサーバ１０を介して双方向通信が可能な形態で接続して構成される。

【００１１】セキュリティサーバ２０、セキュリティサーバ３０は、例えば次のような２つの条件を満たすデータのみの透過を許容する機能を備えた、公知のものである。

（１）ホームページへの接続に用いるＨＴＴＰまたは電子メールの交換に用いられるＳＭＴＰに従うデータであること、（２）配下のクライアントから自サーバを通して外部ネットワーク、例えばインターネット上にあるホームページサーバにホームページデータを要求したとき

に、当該要求に応じてそのホームページサーバから返信されたデータであること。なお、本実施形態では、上記条件を満たす形態のデータを「透過許容データ」と称する。図１の参照符号ＩＬは、この透過許容データによって仮想的に形成される通信経路である。

【００１２】通常、セキュリティサーバ２０が、配下のクライアント２０ａ～２０ｎのいずれかとセキュリティサーバ３０の配下のクライアント３０ａ～３０ｎのいずれかとの間でセッションを確立しようとしても、上記透過許容データ以外のデータの場合は、セキュリティサーバ３０によってセッション確立が拒否される。そこで本実施形態では、リレーサーバ１０で、データ通信を行うクライアント間に擬似的な透過許容データの通信経路ＩＬを形成し、リアルタイム通信またはそれに近似した通信を行えるようにする。

【００１３】このような機能を実現するためのリレーサーバ１０の機能ブロック構成を示したのが、図２である。このリレーサーバ１０では、自サーバを介してデータ通信を行うクライアントの識別情報、各クライアントを配下にもつ（各クライアントを保護する）セキュリティサーバの識別情報、このセキュリティサーバによる上記透過許容データをデータベース部１５０へ登録しておく。例えば、クライアント２０ａがクライアント３０ａと通信を行う場合は、クライアント２０ａ、クライアント３０ａ、セキュリティサーバ２０、セキュリティサーバ３０の識別情報を登録しておく。

【００１４】登録は、以下のようにして行う。例えばクライアント３０ａからクライアント３０ａ宛のデータ送信要求が送信されたとする。リレーサーバ１０は、このデータ送信要求をＩ／Ｏインターフェース１１０を介して受信し、登録・通信要求受付部１２０でこれを受け付けて判断処理部１３０に渡す。判断処理部１３０は、クライアント２０ａが登録が可能かどうかを調べ、可能であれば、ＩＤ発行部１４０に通知する。ＩＤ発行部１４０は、クライアント２０ａ用にユニークなＩＤを発行し、これを識別情報としてデータベース部１５０へ登録する。また、クライアント２０ａを配下にもつセキュリティサーバ２０について、既に識別情報や透過許容データが登録されているかどうかを調べ、未登録であれば、それらを登録する。

【００１５】クライアント２０ａ等が登録された場合は、クライアント２０ａの通信相手先となるクライアント３０ａ及びこれを配下とするセキュリティサーバ３０が登録されているかどうかを調べる。未登録の場合は上述の場合と同様の手順によってユニークなＩＤや透過許容データを登録する。クライアント３０ａ等が登録された場合、あるいは既に登録されていた場合は、セッション確立部１８０でクライアント２０ａとクライアント３０ａとの間のセッションを確立する。

【００１６】その後、クライアント２０ａから通信データが送信されてきた場合は、これを登録・通信要求部１２０で受け付け、データ管理部１７０でクライアント毎に管理する。このとき、データ送信部１６０は、通信相手先のクライアント３０ａに当該クライアント宛の通信データがあることを通知する。クライアント３０ａから要求があった場合は、データ管理部１７０でセキュリティサーバ３０の透過許容データに適合するようにデータを擬似的に変換し、そのデータをクライアント３０ａ宛に送信する。

【００１７】透過許容データへの擬似的な変換は、クライアント３０ａ宛の通信データのヘッダ部に、例えば以下のような情報を付加することにより行う。

（１）その通信データがクライアント３０ａが要求したホームページサーバからの返信データである旨の情報、

（２）その通信データの形態が、セキュリティサーバ３０の透過許容データ、例えば、ホームページデータ又は電子メールの形態である旨の情報。これにより、セキュリティサーバ３０は、渡された通信データが、自サーバの配下にあるクライアント３０ａが要求したデータの返信であると認識するので、その通信データは排除されることなく、クライアント３０ａへ転送される。

【００１８】なお、図示を省略したが、データ管理部１７０には、セッションが確立されたクライアント専用のバッファ領域がそれぞれ確保されており、各クライアントにとって、自分の記憶装置であるかのような取り扱いを可能にしている。例えば、クライアント２０ａ用のバッファ領域に通信データを蓄積しておき、クライアント３０ａからの要求時にこれを読み出して随時透過許容データに擬似的に変換するような使用形態、クライアント３０ａ用のバッファ領域に予め擬似的に透過許容データに変換したデータを格納しておき、クライアント３０ａがこれを随時読みとれるようにする使用形態、クライアント２０ａがクライアント３０ａ用のバッファ領域に直接アクセスして通信データを蓄積し、クライアント３０ａからの要求を契機にこれを随時透過許容データに変換してクライアント３０ａへ送信する使用形態等が可能である。

【００１９】上述のリレーサーバ１０による各機能ブロック１１０～１８０は、通信機能を有するサーバ本体のＣＰＵ（プロセッサ）が、本発明の記録媒体に記録されたプログラムコードを読み取ることによって実現される。記録媒体は、通常、ＣＰＵが随時読み取り可能な固定型ディスクや半導体メモリであるが、フレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＤＶＤ、磁気テープ等の可搬性メディア、あるいはコンピュータがアクセス可能なプログラムサーバ等に記録されて流通し、運用時に上記固定記録媒体にインストールされるものであってもよい。また、ＣＰＵが上記プログラムを実行することによって各機能ブロック１１０～１８０が形成されるだけでなく、その

プログラムの指示に基づいて当該サーバ本体上で稼働しているオペレーティングシステムが実際の処理の一部を行い、その処理を通じて上記各機能ブロック１１０～１８０が形成されるようにしてもよい。

【００２０】次に、図３～図５を参照して上記リレーサーバ１０の機能を説明する。まず、当事者となるクライアント２０ａ，３０ａ、これらを配下とするセキュリティサーバ２０，３０、各セキュリティサーバ２０，３０の透過許容データを予めリレーサーバ１０に登録しておく必要がある。この場合の手順を示したのが図３である。すなわち、クライアント２０ａから、自己とセキュリティサーバ２０の登録要求が発行されると（ステップＳ１０１）、リレーサーバ１０は、その登録受付の可否を判断する。登録受付ができないときは、その旨をクライアント２０ａに通知する（ステップＳ１０２：No、Ｓ１０３）。登録可能なときは、登録要求を発行したクライアント専用のバッファ領域をデータ管理部１７０に確保し（ステップＳ１０２：Yes、Ｓ１０４）、クライアント／セキュリティサーバ用のＩＤを発行する（ステップＳ１０５）。そして、セキュリティサーバ２０の透過許容データをデータベース部１５０に登録する（ステップＳ１０６）。

【００２１】登録後は、図４及び図５に示す手順でデータ通信を開始する。図４において、クライアント２０ａからクライアント３０ａへのデータ送信要求が発行されると（ステップＳ２０１）、リレーサーバ１０は、クライアント２０ａ／セキュリティサーバ２０が登録されており且つ適正なＩＤを所有しているか否かを調べる（ステップＳ２０２）。登録されていなければ拒絶を通知して初期状態に戻る（ステップＳ２０２：Ｎｏ、Ｓ２０３）。登録されている場合は、クライアント２０ａ専用のバッファ領域を確保する（ステップＳ２０４）。その後、クライアント２０ａからの登録一覧送信要求を受け付け、クライアント２０ａに、登録済みのクライアントの一覧を通知する（ステップＳ２０４：Yes、Ｓ２０６）。

【００２２】図５に移り、クライアント２０ａが、登録済みのクライアントの一覧から、クライアント３０ａが既に登録されていることを確認し、そのクライアント３０ａへのデータ送信要求を発行すると（ステップＳ３０１）、リレーサーバ１０は、宛先であるクライアント３０ａが適正か否かを調べる（ステップＳ３０３）。適正でない場合は、データ通信ができない旨をクライアント２０ａに通知し、初期状態に戻る（ステップＳ３０３：No、Ｓ３０４）。適正であれば、クライアント３０ａ専用のバッファ領域を確保するとともに、クライアント２０ａからデータ送信要求があった旨をクライアント３０ａへ通知する（ステップＳ３０５）。

【００２３】その後、クライアント２０ａからの通信データを逐次受信し（ステップＳ３０６）、この受信した通信データをセキュリティサーバ３０の透過許容データに擬似的に変換してクライアント３０ａ専用のバッファ領域に蓄積する。クライアント３０ａから受信要求があったときは、該当するバッファ領域から随時データを読み出してクライアント３０ａ宛に送信する（ステップＳ３０７）。このステップＳ３０６以降の処理をすべての通信データの送信が終了するまで繰り返す（ステップＳ３０８）。

【００２４】なお、クライアント３０ａからクライアント２０ａへのデータ送信要求は、ステップＳ２０１におけるデータ送信要求の主体がクライアント３０ａに置き換えることで実現することができる。このようにして、リアルタイム通信またはそれに近似した通信が可能になる。

【００２５】図６は、本実施形態のデータ通信システムにおいて、あるセキュリティサーバＡの配下にあるクライアントＡから他のセキュリティサーバＢの配下にあるクライアントＢへのデータ通信が、どのような手順で実行されるかを全体的な流れで示したシーケンスチャートである。ここでは、セキュリティサーバＡの透過許容データがＨＴＴＰデータ、セキュリティサーバＢの透過許容データがＳＭＴＰデータであるものとする。リレーサーバは、上述のリレーサーバ１０である。

【００２６】クライアントＡからクライアントＢへのセッション確立が要求されると（Ａ１１）、リレーサーバ１０はその可否を判断し、その結果をクライアントＡへ通知する（Ｃ１１）。セッション確立が許可された場合、クライアントＡは、通信データをエンコードし（Ａ１２）、そのヘッダ部に、通信データがＨＴＴＰ形式であり且つクライアントＢ宛の返信データである旨の情報を付加してデータ送信要求を発行する（Ａ１３）。

【００２７】セキュリティサーバＡは、通信データのヘッダ部から該通信データが透過許容データであるかどうかを審査する。肯定的であれば、リレーサーバ１０に当該通信データを送信する（Ｂ１１）。通信データを受信したリレーサーバ１０は、該通信データをクライアントＢ専用のバッファ領域に通信データを格納し（Ｃ１２）、さらに、クライアントＢに対して送信可能なデータがあることを通知する。

【００２８】通知を受けたクライアントＢは、リレーサーバ１０にデータ受信要求を発行する（Ｆ１１）。このデータ受信要求を受け付けたリレーサーバ１０は、クライアントＢ専用のバッファ領域に記憶されているデータをエンコードし、そのヘッダ部に当該データがクライアントＢの要求に応じて返信するデータである旨の情報と、当該データがＳＭＴＰ形式である旨の情報とを付加し（Ｃ１４）、これをセキュリティサーバＢに送信する（Ｃ１５）。

【００２９】セキュリティサーバＢは、リレーサーバ１０から送信されてきた通信データのヘッダ部を審査して

該通信データが透過許容データ、つまりクライアントＢの要求した返信データであり且つＳＭＴＰ形式であることを確認した後、クライアントＢに、その通信データを転送する（Ｄ１１）。クライアントＢは、その通信データの受信を完了した後、各処理に移行する。

【００３０】このようにして、インターネット上でそれぞれ独立のセキュリティサーバの配下にある２台以上のクライアントについて、セキュリティサーバ及び回線の性能限界範囲でのリアルタイム通信を行うことが可能になる。このようなデータ通信の形態は、インターネットを通じて対戦できる対戦型ゲームサービスやリアルタイムチャットサービス等に広く適用することが可能となる。

【００３１】

【発明の効果】以上の説明から明らかなように、本発明によれば、相手側との間の直接的なデータ通信が制限される環境下においてもリアルタイム通信乃至それに近似した通信を行うことができるという、特有の効果がある。

【図面の簡単な説明】

【図１】本発明を適用したデータ通信システムの構成図。

【図２】本実施形態によるリレーサーバの機能ブロック構成図。

【図３】本実施形態によるリレーサーバへの登録処理手順図。

【図４】本実施形態によるクライアント間のデータ通信の処理手順図。

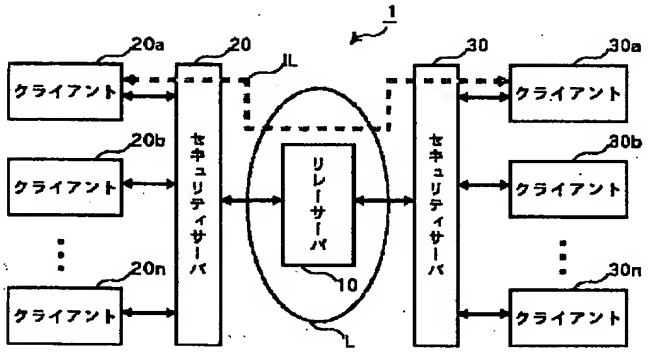
【図５】本実施形態によるクライアント間のデータ通信の処理手順図。

【図６】全体的なデータ通信の処理の流れを示したシーケンスチャート。

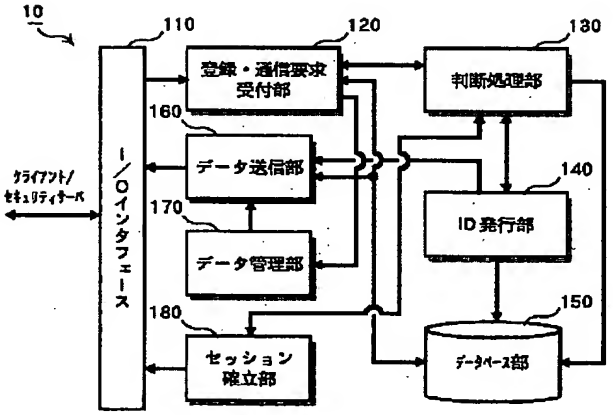
【符号の説明】

１　　データ通信システム
１０　リレーサーバ
１１０　Ｉ／Ｏインターフェース
１２０　登録・通信要求部
１３０　判断処理部
１４０　ＩＤ発行部
１５０　データベース部
１６０　データ送信部
１７０　データ管理部
１８０　セッション確立部

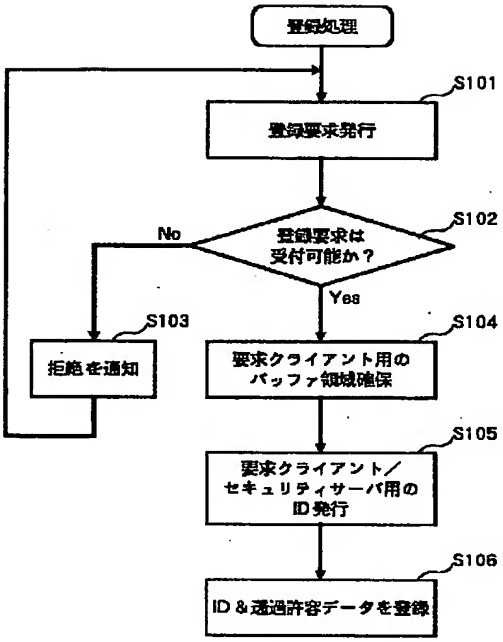
【図１】



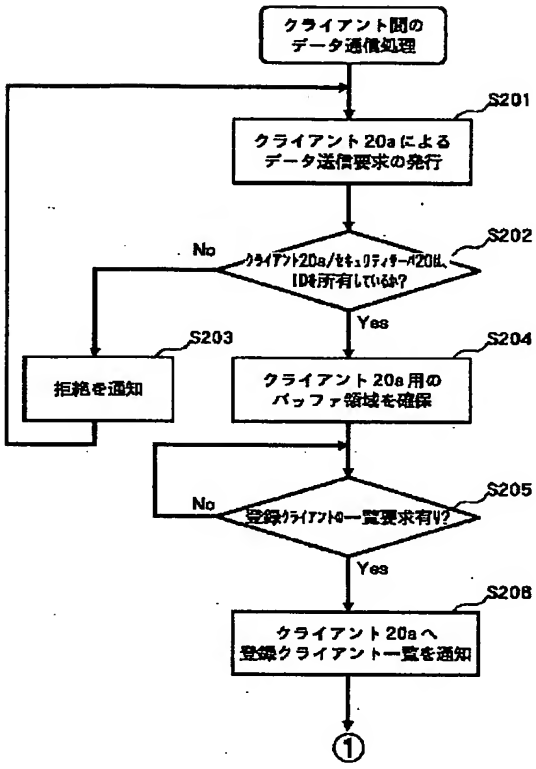
【図２】



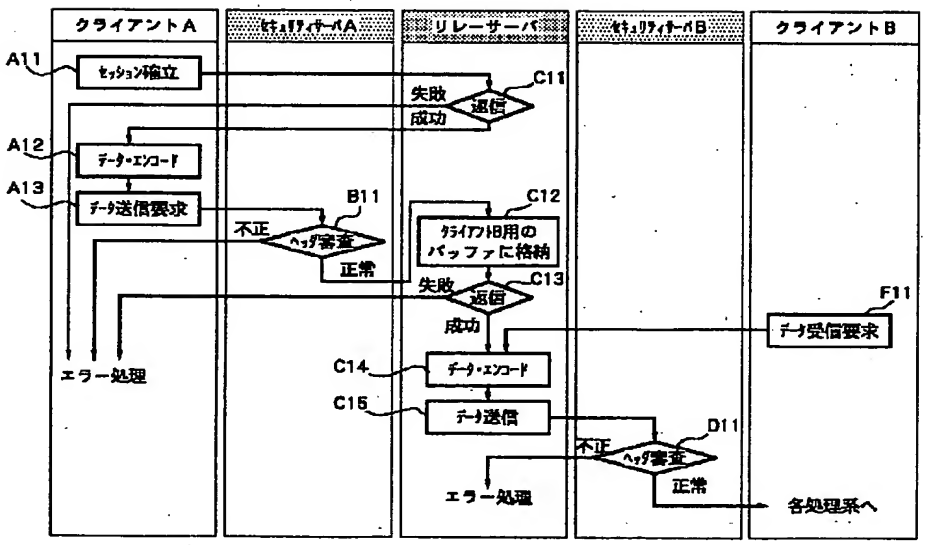
【図３】


登録処理
S101
登録要求発行
S102
No
登録要求は
受付可能か？
Yes
S103
拒絶を通知
S104
要求クライアント用の
バッファ領域確保
S105
要求クライアント／
セキュリティサーバ用の
ID発行
S106
ID＆通過許容データを登録

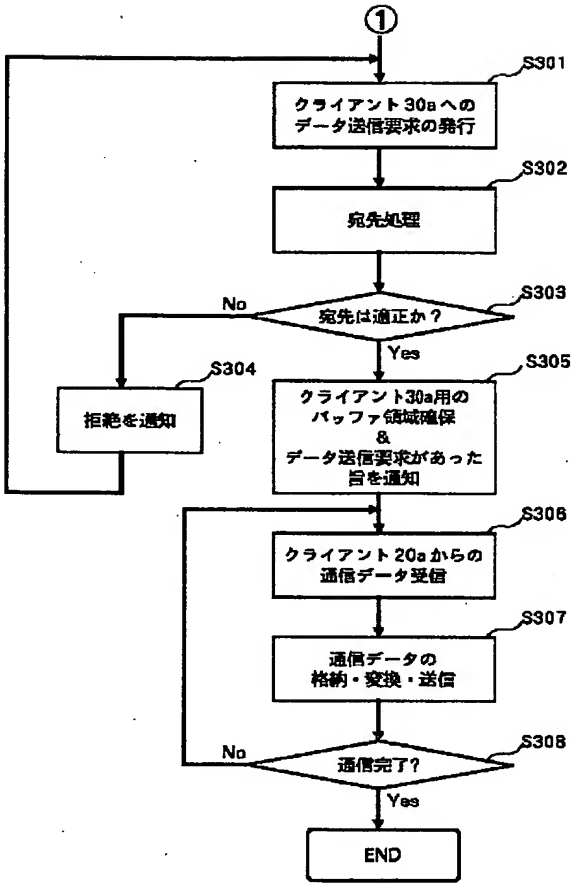
【図４】


クライアント間の
データ通信処理
S201
クライアント20aによる
データ送信要求の発行
S202
No
クライアント20a/セキュリティサーバ20Bは、
IDを所有しているか?
Yes
S203
拒絶を通知
S204
クライアント20a用の
バッファ領域を確保
S205
No
登録クライアント一覧要求有り?
Yes
S206
クライアント20aへ
登録クライアント一覧を通知
①

【図６】


クライアントA
セキュリティサーバA
リレーサーバ
セキュリティサーバB
クライアントB
A11
セッション確立
失敗
成功
C11
返信
A12
データ・エンコード
A13
データ送信要求
B11
不正
ヘッダ審査
正常
C12
クライアントB用の
バッファに格納
失敗
C13
返信
成功
F11
データ受信要求
エラー処理
C14
データ・エンコード
C15
データ送信
D11
不正
ヘッダ審査
正常
エラー処理
各処理系へ

【図５】



【手続補正書】
【提出日】平成１１年８月２７日（１９９９．８．２７）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　配下にある１又は複数の通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置が介在する環境下で行うデータ通信方法であって、
前記セキュリティ装置と外部装置との間にデータ中継装置を介在させ、
このデータ中継装置で、外部装置から特定の前記通信装置宛の適正なＩＤが付された通信データを前記透過許容データに擬似的に変換して当該セキュリティ装置を透過させることを特徴とする、データ通信方法。
【請求項２】　前記外部装置、セキュリティ装置及び前記特定の通信装置をそれぞれ登録しておき、登録された外部装置から登録された通信装置宛の通信データのみを前記透過許容データに擬似的に変換して前記登録されたセキュリティ装置を透過させることを特徴とする、請求項１記載のデータ通信方法。
【請求項３】　それぞれ配下にある１又は複数の通信装置との間で所定形態の透過許容データのみの透過を許容する複数のセキュリティ装置が介在する環境で行うデータ通信方法であって、
一のセキュリティ装置と他のセキュリティ装置との間にデータ中継装置を介在させ、
このデータ中継装置で、一のセキュリティ装置の配下にある第１通信装置から他のセキュリティ装置の配下にある第２通信装置宛の適正なＩＤが付された通信データを当該他のセキュリティ装置用の前記透過許容データに擬似的に変換して当該他のセキュリティ装置を透過させることを特徴とする、データ通信方法。
【請求項４】　前記通信データまたは透過許容データを前記第２通信装置毎に一時的に保持しておき、前記第２

通信装置からの要求を契機に当該通信データについてはそれを前記他のセキュリティ装置用の透過許容データに擬似的に変換し、当該透過許容データについてはそれを当該第２通信装置宛に送信することを特徴とする、請求項３記載のデータ通信方法。

【請求項５】　配下にある通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置と外部装置との間に介在し、

前記外部装置、前記セキュリティ装置及びこのセキュリティ装置の配下にある相手側通信装置を登録する登録手段と、

前記登録された外部装置から前記登録された相手側通信装置宛の通信データを登録された前記セキュリティ装置用の透過許容データに擬似的に変換するデータ変換手段と、

前記擬似的に変換された透過許容データを前記セキュリティ装置を介して前記登録された相手側通信装置に導く手段とを備えて成る、データ中継装置。

【請求項６】　前記相手側通信装置毎のデータ記憶領域を有し、前記通信データ変換手段は、保持されている前記通信データを前記相手側通信装置からの要求を契機に前記透過許容データに擬似的に変換することを特徴とする、

請求項５記載のデータ中継装置。

【請求項７】　前記データ変換手段は、前記通信データのヘッダ部分に、当該通信データが前記相手側通信装置からの要求に応じたものであり且つＨＴＴＰまたはＳＭＴＰに従うデータである旨の情報を付加することで当該通信データを擬似的に前記透過許容データに変換することを特徴とする、

請求項６記載のデータ中継装置。

【請求項８】　前記外部装置が、前記セキュリティ装置と同種の機能を有する他のセキュリティ装置の配下にある通信装置であることを特徴とする、

請求項５記載のデータ中継装置。

【請求項９】　前記セキュリティ装置及び前記他のセキュリティ装置と共に、ＴＣＰ／ＩＰに準拠した公衆通信網に接続されることを特徴とする、

請求項８記載のデータ中継装置。

【請求項１０】　配下にある通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置と外部装置の各々に対するデータ通信機能を具備したコンピュータ装置に、少なくとも、

前記外部装置、前記セキュリティ装置及びそのセキュリティ装置の配下にある相手側通信装置を登録する処理と、

前記登録された外部装置から前記登録された相手側通信装置宛の通信データを擬似的に前記透過許容データに変換する処理と、

前記擬似的に変換された透過許容データを前記セキュリティ装置を介して前記登録された相手側通信装置に導く処理とを実行させるためのプログラムが記録された、コンピュータ読取可能な記録媒体。

【手続補正２】

【補正対象書類名】明細書

【補正対象項目名】０００５

【補正方法】変更

【補正内容】

【０００５】

【課題を解決するための手段】上記課題を解決する本発明のデータ通信方法は、配下にある１又は複数の通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置が介在する環境下で行うデータ通信方法であって、セキュリティ装置と外部装置との間にデータ中継装置を介在させ、このデータ中継装置で、外部装置から特定の前記通信装置宛の適正なＩＤが付された通信データを前記透過許容データに擬似的に変換して当該セキュリティ装置を透過させることを特徴とする。好ましくは、前記セキュリティ装置及び前記特定の通信装置を予め登録しておき、登録した通信装置宛の通信データのみを前記透過許容データに擬似的に変換して登録されたセキュリティ装置を透過させるようにする。

【手続補正３】

【補正対象書類名】明細書

【補正対象項目名】０００６

【補正方法】変更

【補正内容】

【０００６】前記セキュリティ装置が複数介在する環境でデータ通信を行う場合は、前記データ中継装置をセキュリティ装置間に介在させ、特定のセキュリティ装置の配下にある第１通信装置から他のセキュリティ装置の配下にある第２通信装置宛の適正なＩＤが付された通信データを当該他のセキュリティ装置用の前記透過許容データに擬似的に変換して当該他のセキュリティ装置を透過させる。なお、前記通信データまたは透過許容データを前記第２通信装置毎に一時的に保持しておき、前記第２通信装置からの要求を契機に当該通信データについてはそれを前記他のセキュリティ装置用の透過許容データに擬似的に変換し、前透過許容データについてはそれを当該第２通信装置宛に送信するようにしてもよい。

【手続補正４】

【補正対象書類名】明細書

【補正対象項目名】０００７

【補正方法】変更

【補正内容】

【０００７】上記他の課題を解決する本発明のデータ中継装置は、配下にある通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置と外部装置との間に介在するもので、前記外部装置、前記セキュリティ装置及びこのセキュリティ装置の配下にある

相手側通信装置を登録する登録手段と、前記登録された外部装置から前記登録された相手側通信装置宛の通信データを擬似的に登録された前記セキュリティ装置用の透過許容データに変換するデータ変換手段と、前記擬似的に変換された透過許容データを前記セキュリティ装置を介して前記登録された相手側通信装置に導く手段とを備えて構成したものである。

【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】０００９
【補正方法】変更
【補正内容】
【０００９】上記他の課題を解決する本発明の記録媒体は、配下にある通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置と外部装置の各々に対するデータ通信機能を具備したコンピュータ装置に、少なくとも下記の処理を実行させるためのプログラムが記録された、コンピュータ読取可能な記録媒体である。

（１）前記外部装置、前記セキュリティ装置及びそのセキュリティ装置の配下にある相手側通信装置を登録する処理、

（２）前記登録された外部装置から前記登録された相手側通信装置宛の通信データを擬似的に前記透過許容データに変換する処理、

（３）前記擬似的に変換された透過許容データを前記セキュリティ装置を介して前記登録された相手側通信装置に導く処理。

フロントページの続き

(72)発明者　川上　量生
東京都中央区日本橋人形町２丁目13番９号　ＢＲ人形町１ビル３階　株式会社ドワンゴ内

Ｆターム(参考)　5K030 GA15 HA05 HD01 JT02 LC13 LD19 LD20
9A001 LL03